多値論理関数のカスケード合成 (多値論理およびその応用 II)

AUTHOR(S):

原尾, 政輝; 野口, 正一; 大泉, 充郎

CITATION:

原尾, 政輝 ...[et al]. 多値論理関数のカスケード合成 (多値論理およびその応用 II). 数理解析研究所講究録 1972, 140: 111-135

ISSUE DATE:

1972-04

URL:

http://hdl.handle.net/2433/106675

数理解析研究所講究録
140巻 1972年 111-135

多値論理関数のカスケード合成

原尾 政輝　　野口 正一　　大泉 充郎
（東北大学大学院）（東北大学電気通信研究所）

はじめに　多値論理の研究はその関数の完備性を調べるものと、それらによって表現された関数を如何に実現するかということがある。前者については色々な論理系が考案されているが、2値の場合のブール演算がリレー回路に対応したようにそのまま演算系が回路素子やトポロジーと対応するとは言えない。ここではXを位数が素数pのn乗 p^n であると仮定した時、GF(p^n)の演算を導入する。すると多値関数 $f: X^n \to X$ はGF(p^n)の演算を用いて一意的に表現することができる。Maisel[4]はこのような形の論理関数についてリレー回路で合成する方法を述べている。ここでは最近の回路網の集積化に伴って重要視されている反復回路網で合成する問題を取り扱かう。まず作用素の概念を導入し、任意の多出力回路網が数種のセルのカスケードで合成できることを示す。又この手法はGF(p)で定義された回路網合成理論[6]の一般化であり、GF(p)の場合の結果と比較するために最後にGF(p)の場合の主な結果についてのべる。

1. 関数の表現

1.1. $GF(p^m)$ の演算と展開公式

$GF(p)$ の上の次数 m の多項式を

$$p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$$

とおくとき、$R_{p(x)}$ を modulo $p(x)$ での多項式環とする。特に $P(x)$ が既約多項式であれば $R_{p(x)}$ は体をなし、これを $GF(p^m)$ とよんでいる。良く知られているように、すべての有限体は $GF(p^m)$ と同型である。いま X を有限集合で位数が p の巾（p は素数）p^m であれば、任意の写像 $f: X^n \to X$ は $GF(p^m)$ の演算を用いて完全に記述することができる。

記法.1 $GF(p^m)$ の元を真理値に対応させ、これを $X = \{\alpha_0, \alpha_1, \cdots, \alpha_{p^m-1}\}$ とする。又 $GF(p^m)$ の加法及び乗法を2値環和表現に対応させ"⊕"，"・"で表わし、このように定義された代数系を論理系 $\langle X, \oplus, \cdot \rangle$ とよぶ。特に X の単位元および零元を 1，0 で表わす。

この $GF(p^m)$ の演算で定義された代数系は、結合、分配、交換律を満す分配系であり、論理系 $\langle X, \oplus, \cdot \rangle$ は完備である。つぎにこの系の一般展開公式を導くために2，3の定義を与えよう。

定義・1　一変数関数　$J_{\alpha_i} : X \to X$　で次の条件を満すものを基底関数と定義する；

$$J_{\alpha_i}(x) = \begin{cases} 1 & \text{if } x = \alpha_i \\ 0 & \text{otherwise} \end{cases} \qquad \text{—(1)}$$

いま変数を x とするとき，$\overbrace{x \cdot x \cdot \cdots \cdot x}^{i} = x^i$，$\alpha_i x^\varepsilon \oplus \alpha_j x^\varepsilon = (\alpha_i \oplus \alpha_j) x^\varepsilon$ 等と書くことにする。

定理・1　基底関数 $J_{\alpha_i}(x)$ はつぎのように表わされる；

$$J_{\alpha_i}(x) = \ominus x\,(x \ominus 1)(x \ominus \alpha_2) \cdots (x \ominus \alpha_{i-1})(x \ominus \alpha_{i+1}) \cdots (x \ominus \alpha_{p^m-1}) \qquad \text{—(2)}$$

ただし $\ominus x$ は x の加法についての逆元とする。

(証明)

$$x^{p^m-1} \ominus 1 = \prod_{i=1}^{p^m-1} (x \ominus \alpha_i) \quad \text{だから}$$

$$\ominus 1 = (\ominus \alpha_1)(\ominus \alpha_2) \cdots (\ominus \alpha_{p^m-1})$$

$$J_{\alpha_i}(\alpha_i) = \ominus \alpha_i\,(\alpha_i \ominus 1)(\alpha_i \ominus \alpha_2) \cdots (\alpha_i \ominus \alpha_{i-1})(\alpha_i \ominus \alpha_{i+1}) \cdots (\alpha_i \ominus \alpha_{p^m-1})$$

において．加法演算の下で $x \ominus \alpha_i$ は推移的だから．各項 $\alpha_i \ominus \alpha_j$ は $\alpha_i \ominus \alpha_i$ の項を除いて相異なる $GF(p^m)$ の元をとる。上の式より相異なる元の積は $\ominus 1$ より $J_{\alpha_i}(\alpha_i) = 1$

を得る。 $x \neq a_i$ であれば項 $x \ominus a_i$ が零となるから

$J_{a_i}(a_j) = 0$ $\quad$ if $i \neq j$ $\quad$ (証明終)

又単位元 1 は中等元であるから $J_{a_i}^{k}(x) = J_{a_i}(x)$. しかも唯一の真理値に対して $J_{a_i}(x)$ は真理値 1 をとるので次が成りたつ;

定理.2 基底関数には次の関係が成立する;

$$J_{a_i}(x) \cdot J_{a_j}(x) = \begin{cases} 0 & \text{if } a_i \neq a_j \\ J_{a_i}(x) & \text{if } a_i = a_j \end{cases}$$

$$\sum_{i=0}^{p^m-1} J_{a_i}(x) = 1$$

以上まとめると、この論理系は $\oplus$ 演算の下で線形空間をつくっており、一変数の場合は $J_{a_i}(x)$ がその基底に相当していると考えることができる。今n変数関数の集合を $\mathcal{F}_n = \{ f \mid f : X^n \to X \}$ とおくと、この関数集合が又 $\oplus$ 演算の下で線形空間をつくっていることが考えられ、$\mathcal{F}_n$ の基底に相当する関数を求めることが肝要になる。

定義・2　変数 x_i に関する基底関数を $J_{\rho i}(x_i)$ で表わすとき、つぎの n 変数関数を最小項関数と定義する；

$$m_k(x_1, x_2, \cdots, x_n) = J_{\rho k_1}(x_1) \cdot J_{\rho k_2}(x_2) \cdot \cdots \cdot J_{\rho k_n}(x_n) \quad -(3)$$

この最小項関数の集合 $\{m_k\}$ が $\mathcal{F}_n$ の基底に対応するもので、次の性質を満しているコトが分る；

定理・3.　最小項関数間には次の関係が成立する：

(i)　$m_i(x_1, x_2, \cdots, x_n) \cdot m_j(x_1, x_2, \cdots, x_n)$

$$= \begin{cases} 0 & \text{if } i \neq j \\ m_i(x_1, x_2, \cdots, x_n) & \text{if } i = j \end{cases}$$

(ii)　$$\sum_{i=0}^{p^{mn}-1} m_i(x_1, x_2, \cdots, x_n) = \mathbb{1}$$

(証明略)

最小項関数 $m_k(x_1, x_2, \cdots, x_n)$ は X^n の元 $k = (\rho_{k_1}, \rho_{k_2}, \cdots, \rho_{k_n})$ に対してのみ真理値1をとるブール関数の最小項に対応する関数である。多値関数 $f: X^n \to X$ が与えられた時、その展開公式が重要であるが、2値関数の最小項展開の一般化として、最小項関数を用いた展開公式が得られる。

定理. 4. 任意の p^m 値関数を $f: X^n \to X$ とする。X^n の元 $k = (\alpha_{k1}, \alpha_{k2}, \cdots, \alpha_{kn})$ に対して $f(k) = \beta_k$ ならば f はつぎのように展開される：

$$f(x_1, x_2, \cdots, x_n) = \sum_{k=0}^{p^{mn}-1} \beta_k \, J_{k_1}(x_1) \cdot J_{k_2}(x_2) \cdot \cdots \cdot J_{k_n}(x_n)$$

$$= \sum_{j=0}^{p^{mn}-1} \beta_j \, m_j(x_1, x_2, \cdots, x_n) \quad -(4)$$

（証明） $\mathcal{F}_n$ は $GF(p^m)$ の元を係数，$\{m_k(x_1, \cdots, x_n)\}$ を基底とする p^{mn} 次元のベクトル空間とみなせるから，$\mathcal{F}_n$ の任意の元は演算"$\oplus$"に関する一次結合で一意的に表わされねばならない。 （証明終）

展開式（4）の各最小項関数を式（2）を用いて展開してやる。すると各項は $1, \cdots, p^{m}-1, x_1, \cdots, x_1^{p^m-1}, \cdots, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}, \cdots, x_1^{p^m-1} \cdots x_n^{p^m-1}$ の形の項の一次結合に分解される。即ち

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{p^{mn}-1} \gamma_i \, x_1^{\varepsilon_{i_1}} x_2^{\varepsilon_{i_2}} \cdots x_n^{\varepsilon_{i_n}} \quad -(5)$$

ただし $\gamma_i \in GF(p^m)$, $\varepsilon_{i_j} \in \mathbb{Z}/p^m$

特に $x^0 = 1$ とおく。(5) 式は各項 $\{ x_1^{\varepsilon_{i_1}} x_2^{\varepsilon_{i_2}} \cdots x_m^{\varepsilon_{i_m}} \}$ を基底とする加群である。(4) 式による表現を最小項関数表示，(5) 式によるものを ELF 表示とよぶ。

1.2. 展開式間の関係

最小項関数 $m_i(x_1, \cdots, x_n) = J_{i_1}(x_1) \cdot J_{i_2}(x_2) \cdots J_{i_m}(x_m)$ のとき $i = i_1 + p^m i_2 + \cdots + p^{m(m-1)} i_m$ とする。この最小項関数の順序組を次のようにおく：

$$M_m = (m_0, m_1, \cdots, m_{p^{mm}-1})$$

同様に (5) 式の基底の順序組を

$$B_m = (1, x_1, x_1^2, \cdots, x_1^{p^{m-1}} x_2^{p^{m-1}} \cdots x_n^{p^{m-1}})$$

とおく。この基底間の関係について調べてみる。いま基底関数間の変換 (2) 式を

$$M_1^T = \begin{bmatrix} J_0(x) \\ J_1(x) \\ J_2(x) \\ \vdots \\ J_{p^m-1}(x) \end{bmatrix} = \begin{bmatrix} & & \\ & (d_{ij}) & \\ & & \end{bmatrix} \begin{bmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{p^m-1} \end{bmatrix} = D_1 \cdot B_1^T$$

と表わすと、一般には次の性質をもつ。

定理 5　論理系 $\langle X, \oplus, \cdot \rangle$ の一変数関数に $M_1^T = D_1 \cdot B_1^T$ が成りたてば、n 変数関数関には、関係

$$M_n^T = D_n \cdot B_n^T$$

がある。ここで $\otimes$ を Kronecker 積とすれば

$$D_n = D_1 \otimes D_{n-1} = \begin{bmatrix} d_{ij} D_{n-1} \end{bmatrix}$$

（証明）　$n = k$ までは証明されたとしよう。　$n = k+1$ では各最小項関数は $p^{m_{k+1}} = \gamma$ とおくと、

$$0 \le i \le \gamma - 1 \Rightarrow m_i(x_1, x_2, \cdots, x_{k+1}) = m_i(x_1, \cdots, x_k)$$

$$\cdot J_0(x_{k+1}) = d_{00} m_i(x_1, \cdots, x_k) \oplus d_{01} m_i(x_1, \cdots, x_k) x_{k+1} \oplus \cdots \oplus d_{0 p^{m_{k+1}}-1} m_i(x_1, \cdots, x_k) \cdot x_{k+1}^{p^{m_{k+1}}-1}$$

$M_k^T = D_k \cdot B_k^T$ なる関係があるから

$$\begin{bmatrix} m_0 \\ m_1 \\ \vdots \\ m_{\gamma-1} \end{bmatrix} = \begin{bmatrix} [d_{00} D_k], [d_{01} D_k], \cdots, [d_{0 p^{m_{k+1}}-1} D_k] \end{bmatrix} \begin{bmatrix} [B_k] \\ [B_k x_{k+1}] \\ \vdots \\ [B_k x_{k+1}^{p^{m_{k+1}}-1}] \end{bmatrix}$$

同様にして

$(s-1)\gamma \leq i \leq s\cdot\gamma - 1 \Rightarrow m_i(x_1, x_2, \cdots, x_{k+1}) = m_{i-(s-1)\gamma}(x_1, x_2, \cdots, x_k) \cdot J_s(x_{k+1}) = \alpha_{s0}\, m_i(x_1, \cdots, x_{k+1}) \oplus \alpha_{s1}\, m_i(x_1, \cdots, x_k)\cdot x_{k+1} \oplus \cdots \oplus \alpha_{sp^m-1} \cdot m_i(x_1, \cdots, x_k)\, x_{k+1}^{p^m-1}$

故に行列形に直せば

$$D_{k+1} = D_1 \otimes D_k$$

(証明終)

例題・1　GF(3) での基底変換

1	x	x^2
1	0	0
1	1	1
1	2	1

$J_0(x) = 1 \oplus 2x^2$

$J_1(x) = 2x \oplus 2x^2$

$J_2(x) = x \oplus 2x^2$

故に $\begin{bmatrix} J_0 \\ J_1 \\ J_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ x^2 \end{bmatrix} = D_1 \cdot B_1$

したがって

$$D_2 = \begin{bmatrix} D_1 & ① & 2D_1 \\ ① & 2D_1 & 2D_1 \\ ① & D_1 & 2D_1 \end{bmatrix}, \cdots, D_m = \begin{bmatrix} D_{m-1} & ① & 2D_{m-1} \\ ① & 2D_{m-1} & 2D_{m-1} \\ ① & D_{m-1} & 2D_{m-1} \end{bmatrix}$$

ただし、① は 0 行列とする。

系.1　n 変数関数 $f : X^n \to X$ の最小項関数表示及び ELF 表示を

$$f(x_1, \cdots, x_n) = (\beta_0, \beta_1, \cdots, \beta_{p^n-1}) \cdot M_n^T = V_n \cdot M_n^T$$

$$f(x_1, \cdots, x_n) = (\gamma_0, \gamma_1, \cdots, \gamma_{p^n-1}) \cdot B_n^T = R_n \cdot B_n^T$$

とおく。すると $R_n = V_n D_n$

（証明）　定理5より

$$V_n M_n^T = V_n (D_n B_n^T) = (V_n D_n) B_n^T \quad \text{（証了）}$$

系.2　B_n 上の変換を L_n ; $B_n' = L_n B_n$

M_n 上の変換を F_n ; $M_n' = F_n M_n$

とすれば $L_n = D_n^{-1} F_n D_n$

（証明）　$M_n' = D_n B_n' = F_n \cdot D_n B_n$.　$\therefore B_n' = (D_n^{-1} F_n D_n)$

B_n　すなわち　$L_n = D_n^{-1} F_n D_n$.　（証了）

2. 回路網の反復合成

2.1. 回路網の代数表現

ここでいう回路網とは1章で述べた多値関数を合成するもので、図1のように数種のセルのカスケード接続より成っているものとする。又各セルは純組合せ的であるとする。

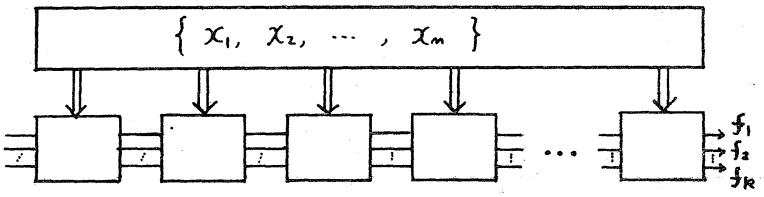


図1

図1に示される k 出力回路網は写像 $f: X^n \to X^k$ とみなすことができる。ここで X^k は rail state を表わす。写像 $f: X^n \to X$ は X に $GF(p^m)$ の演算を定義することによって最小項関数表現ができた。この場合も X^k に適当な演算を導入して写像 $f: X^n \to X^k$ の表現方法を求めたい。今 rail state の集合 X^k にある演算（群演算）を定義したとき H で表わそう。これによって回路網は写像 $f: X^n \to H$ で表わすことができる。このとき s 入力セルは写像 $f: X^s \to H$, 特に 1 入力セルは $\theta: X \to H$ で表わされ、それぞれ図2に対応する。

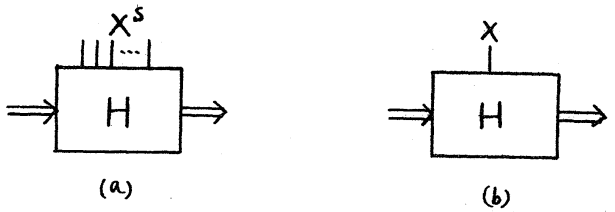


図2.

記法.2 回路網 $f: X^n \to H$ が $i \in X^n$ に対して $f(i) = h_i \in H$ のとき $f = (h_0, h_1, \cdots, h_{p^{mn}-1})_{p^{mn}}$ と書く。この写像の集合を $\mathcal{U}_n$ とおき、この時 s 入力セル $s \leq n$ は $\mathcal{U}_n$ の部分空間をつくるが $\theta = (h_0', h_1', \cdots, h_{p^{mn}-1}')_{p^{mn}}$ 等と $\mathcal{U}_n$ の元として書くことにする。

回路網を合成する場合の目的として (1) セルの個数を最小にする (2) セルの配列を規則的にする (3) セルの種類や構造を簡単にする。等が問題として挙げられるが、ここでは集積化ということを考え、規則的な配列（カスケード）と最簡セルでの実現ということを基本的問題にとり挙げ、1入力セルでの実現問題を考察してゆこう。この時問題になるのは H にどのような演算を定義するかということである。今演算として可換群の演算とその自己準同型演算を定義すれば $\mathcal{U}_n$ は多元環をなす。特に回路網の各セルへの入力と $f: X^n \to H$ の展開形が1対1に対応するように定めてある。即ち次の関係を満すように定める：

$$f(X^n) = (h_0, h_1, h_2, \cdots, h_{p^{mn}-1})$$
$$g(X^n) = (h_0', h_1', h_2', \cdots, h_{p^{mn}-1}')$$

$$\Rightarrow f(X^n) \oplus g(X^n) = (f \oplus g)(X^n)$$
$$= (h_0 \oplus h_0', h_1 \oplus h_1', \cdots, h_{p^{mn}-1} \oplus h_{p^{mn}-1}')$$

$$f(X^n)\cdot g(X^n) = (f\cdot g)(X^n)$$
$$= (h_0\cdot h_0',\ h_1\cdot h_1',\ \cdots,\ h_{p^{mn}-1}\cdot h_{p^{mn}-1}')$$

このような演算を満すものとして、特に $GF(p^m)$ の上の k 次元ベクトルをとろう。すると次に示すように最小項関数表示と類似の展開公式を得る。

<u>定理 6</u>　回路網 $f: X^n \to GF(p^m)^k$ は $i \in X^k$ に対する真理値を $f(i) = t_i \in GF(p^m)^k$ とおけば次のように展開される;

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{p^{mn}-1} t_i\, m_i(x_1, x_2, \cdots, x_n) \quad — (6)$$

(略証)　この写像 f の集合 $\mathcal{U}_n$ は $GF(p^m)^k$ の上の $\{m_i(x_1, x_2, \cdots, x_n)\}$ を基底とするベクトル空間とみなすことができるから任意の $\mathcal{U}_n$ の元はこれらの基底の一次結合として一意的に表わされる。これが (6) である。　(証明終)

いま $t_i \in GF(p^m)^k$ を $GF(p^m)$ の元を成分とする k-tuple で表わす。それらの演算は成分毎の加法及び乗法として次のように定義される;

$$t_i = (t_{i1}, t_{i2}, \cdots, t_{ik})$$
$$t_j = (t_{j1}, t_{j2}, \cdots, t_{jk})$$

$$\Rightarrow\ t_i \oplus t_j = (t_{i1}\oplus t_{j1},\ t_{i2}\oplus t_{j2},\ \cdots,\ t_{ik}\oplus t_{jk})$$

$$t_{i_1} \cdot t_j = (t_{i_1} \cdot t_{j1},\ t_{i_2} \cdot t_{j2},\ \cdots,\ t_{ik} \cdot t_{jk})$$

又 $(t_{i1}, t_{i2}, \cdots, t_{ik})\, m_i = (t_{i1} m_i,\ t_{i2} \cdot m_i, \cdots, t_{ik} m_i)$

とおけば (6) 式は

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{p^{mn}-1} (t_{i1} m_i,\ t_{i2} m_i, \cdots, t_{ik} m_i)$$

$$= (\mathcal{X}_1,\ \mathcal{X}_2, \cdots, \mathcal{X}_k).$$

ここで $\mathcal{X}_i$ は i 成分についての最小項関数表示であるとする。

更に上の関係を用いて最小項関数を展開すれば

$$f(x_1, x_2, \cdots, x_n) = \Big(\sum_{i=0}^{p^{mn}-1} \gamma_{i1}\, x_1^{\varepsilon_{i11}} \cdots x_n^{\varepsilon_{i1n}},\ \sum_{i=0}^{p^{mn}-1} \gamma_{i2}\, x_1^{\varepsilon_{i21}} \cdots x_n^{\varepsilon_{i2n}},\ \cdots,\ \sum_{i=0}^{p^{mn}-1} \gamma_{ik}\, x_1^{\varepsilon_{ik1}} \cdots x_n^{\varepsilon_{ikn}} \Big)$$

$$= \sum_{j=0}^{p^{mn}-1} (\gamma_{j1}, \gamma_{j2}, \cdots, \gamma_{jk})\, x_1^{\varepsilon_{j1}} x_2^{\varepsilon_{j2}} \cdots x_n^{\varepsilon_{jn}} \quad -(7)$$

(6) 式及び (7) 式をそれぞれ回路網 $f : X^n \Rightarrow H$ の最小項関数表示及び ELF 表示とよぶ。

<u>例題 2</u> 次の関数の ELF 表示を求めよ.

x_1	0 1 s_1 s_2	0 1 s_1 s_2	0 1 s_1 s_2	0 1 s_1 s_2
x_2	0 0 0 0	1 1 1 1	s_1 s_1 s_1 s_1	s_2 s_2 s_2 s_2
H	1 p_1 0 p_2	0 0 0 s_1	0 s_2 0 s_2	1 0 0 0
	0 s_2 0 1	1 0 0 1	0 0 0 1	s_2 0 s_1 0

GF(2^2) の演算は $p(x) = x^2 + x + 1$ とおくと次のようになる。

+	0	1	ρ_1	ρ_2
0	0	1	ρ_1	ρ_2
1	1	0	ρ_2	ρ_1
ρ_1	ρ_1	ρ_2	0	1
ρ_2	ρ_2	ρ_1	1	0

·	0	1	ρ_1	ρ_2
0	0	0	0	0
1	0	1	ρ_1	ρ_2
ρ_1	0	ρ_1	ρ_2	1
ρ_2	0	ρ_2	1	ρ_1

従って基底関数は

$$J_0(x) = x^3 \oplus 1, \quad J_1(x) = x^3 \oplus x^2 \oplus x$$

$$J_{\rho_1}(x) = x^3 \oplus \rho_1 x^2 \oplus \rho_2 x, \quad J_{\rho_2}(x) = x^3 \oplus \rho_2 x^2 \oplus \rho_1 x.$$

$$\begin{aligned} f(x_1, x_2) &= (1, 0)\, J_0(x_1) \cdot J_0(x_2) \oplus (\rho_1, \rho_2)\, J_1(x_1) \cdot J_0(x_2) \\ &\oplus (\rho_2, 1)\, J_{\rho_2}(x_1) \cdot J_0(x_2) \oplus (0, 1)\, J_0(x_1) \cdot J_1(x_2) \\ &\oplus (\rho_1, 1)\, J_{\rho_2}(x_1) \cdot J_1(x_2) \oplus (\rho_2, 0)\, J_1(x_1) \cdot J_{\rho_1}(x_2) \\ &\oplus (\rho_2, 1)\, J_{\rho_2}(x_1) \cdot J_{\rho_1}(x_2) \oplus (1, \rho_2)\, J_0(x_1) \cdot J_{\rho_2}(x_2) \\ &\oplus (0, \rho_1)\, J_{\rho_1}(x_1) \cdot J_{\rho_2}(x_2) \end{aligned}$$

$$\begin{aligned} = (\, &1 \oplus \rho_2 x_1^3 x_2^3 \oplus x_1^3 x_2^2 \oplus \rho_1 x_1 x_2^3 \oplus \rho_2 x_1 \oplus \rho_2 x_1^2 x_2^2 \\ &\oplus \rho_1 x_1^2 x_2 \oplus \rho_1 x_1 \oplus \rho_1 x_1 x_2 \oplus \rho_2 x_2^2, \quad \rho_1 x_1^3 x_2^3 \oplus x_1^3 x_2^2 \\ &\oplus \rho_2 x_1^2 x_2^3 \oplus \rho_1 x_1 x_2^3 \oplus \rho_1 x_1^3 x_2 \oplus \rho_1 x_1^3 \oplus x_1 \oplus \rho_1 x_2^3 \\ &\oplus x_1 x_2 \oplus \rho_1 x_1 x_2^2 \,) \end{aligned}$$

2.2 回路網の合成

H の演算として $GF(p^m)^k$ をとったから展開式より分るように回路網 $f: X^n \to H$ の表現は k 個の生成元より構成されている。

定義.3 1入力セル $\theta_i : X \to GF(p^m)^k$ であって

$$\theta_i(\alpha) = (0, \cdots, 0, \alpha, 0, \cdots, 0) \in GF(p^m)^k$$

なる関係を満すものを $GF(p^m)^k$ 演算で定義された回路網の成分 i に関する標準セルとよぶ。ここで $0 \leq i \leq k$。

次に回路網の表現形と回路網の対応を考えてみると、ELF表現の項 $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ はセルへの入力を、又係数はそれらのセルの必要個数を示している。更に(7)式における係数の各成分 γ_{ij} は標準セル θ_j を使用することを表わす。

従って1入力セルで回路網を実現するにはELF表現の項の長さを分割する必要があり、そのために乗法演算と回路網との対応を考える。

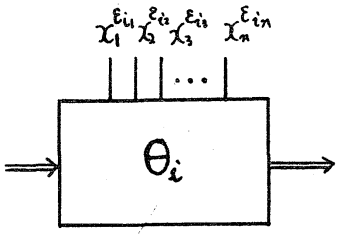


図.3

今 $GF(p^m)$ の加法を群とみなし、その乗法を自己同型作用素とみなす。ある自己同型作用素 g は加法群の置換で表わされ、これを $g(\alpha) = g^{-1} \circ \alpha \circ g$ とかく。ここで g は H の作用素群 G のえで演算 "$\circ$" は $\oplus$ と同一視できる。

又 φ は単位元を除いて推移的な性質をもっている。

定義 4 作用素 $\{\varphi^{(i)}\}$ を成分とする次のセルを作用素セルと定義する*

$$\Phi(x) = (\varphi^{(0)}, \varphi^{(1)}, \cdots, \varphi^{(p^m-1)})_{p^m}.$$

$n-1$ 番数回路網 $f_{n-1}: X^{n-1} \to H$ が与えられたとき，それに入力 x_m をもつセル $\Phi(x_m)$ を施こすことを $\Phi(x_m)\cdot f_{n-1}$ とかく。作用素 $\varphi^{(i)}\cdot\Delta = x_i\cdot\Delta$ なる架法に対応するものとすれば

$$\Phi(x_m)\cdot f_{n-1} = x_0 f_{n-1}\cdot J_0(x_m) \oplus x_1 f_{n-1}\cdot J_1(x_m) \oplus \cdots \oplus x_{p^m-1} f_{n-1}\cdot J_{p^m-1}(x_m) \qquad \text{—— (8)}$$

x_{m-1} ⋯ x_2 x_1	$\Phi(x_m) f_{m-1}$	
0 ⋯ 0 0 0 ⋯ 0 1 ⋮ p^m-1 ⋯ p^m-1 p^m-1	$g_0^{-1}\begin{bmatrix}\Delta_0\\ \Delta_1\\ \vdots\\ \Delta_{p^m-1}\end{bmatrix}$	$g_0 = x_0 f_{m-1}\cdot J_0(x_m)$
0 ⋯ 0 0 0 ⋯ 0 1 ⋮ p^m-1 ⋯ p^m-1 p^m-1	$g_1^{-1}\begin{bmatrix}\Delta_0\\ \Delta_1\\ \vdots\\ \Delta_{p^m-1}\end{bmatrix}$	$g_1 = x_1 f_{m-1}\cdot J_1(x_m)$ —— f_m
⋮	⋮	
0 ⋯ 0 0 0 ⋯ 0 1 ⋮ p^m-1 ⋯ p^m-1 p^m-1	$g_{p^m-1}^{-1}\begin{bmatrix}\Delta_0\\ \Delta_1\\ \vdots\\ \Delta_{p^m-1}\end{bmatrix}$	$g_{p^m-1} = x_{p^m-1} f_{m-1}\cdot J_{p^m-1}(x_m)$

* 詳しくはセル $\Theta = (g_0^{-1}, g_1^{-1}, \cdots, g_{p^m-1}^{-1})$, $\Theta = (g_0, g_1, \cdots, g_{p^m-1})$ の組合せよりなっているが簡単な為このように書く。

いま p^m 個の $(n-1)$-変数関数を $f_{n-1}^0, f_{n-1}^1, \cdots, f_{n-1}^{p^m-1}$ とおき，独立な p^m 個の作用素を $\Phi_0(x_n), \Phi_1(x_n), \cdots, \Phi_{p^m-1}(x_n)$ とする。これらの組合せを

$$f_n = \Phi_0(x_n)\cdot f_{n-1}^0 \oplus \Phi_1(x_n)\cdot f_{n-1}^1 \oplus \cdots \oplus \Phi_{p^m-1}(x_n)\cdot f_{n-1}^{p^m-1} \quad -(9)$$

とおき，(2)式を用いて変数 x_n^i についてまとめる。

$$\begin{aligned} f_n = {} & (g_{00} f_{n-1}^0 \oplus g_{01} f_{n-1}^1 \oplus \cdots \oplus g_{0\,p^m-1} f_{n-1}^{p^m-1}) \\ & \oplus (g_{10} f_{n-1}^0 \oplus g_{11} f_{n-1}^1 \oplus \cdots \oplus g_{1\,p^m-1} f_{n-1}^{p^m-1})\, x_n \\ & \vdots \\ & \oplus (g_{p^m-1\,0} f_{n-1}^0 \oplus g_{p^m-1\,1} f_{n-1}^1 \oplus \cdots \oplus g_{p^m-1\,p^m-1} f_{n-1}^{p^m-1})\, x_n^{p^m-1} \\ = {} & Q_0 \oplus Q_1 x_n \oplus \cdots \oplus Q_{p^m-1} x_n^{p^m-1} \qquad -(10) \end{aligned}$$

(10)式は作用素が定まれば一意的に定まり，これを標準方程式とよぶ。(9)式から(10)式への変換は M_n 基底から B_n 基底への変換であり，D_n が non-singular なことから次の補題を得る；

<u>補題 1</u>　$Q_0, Q_1, \cdots, Q_{p^m-1}$ が与えられたとき，$f_{n-1}^0, f_{n-1}^1, \cdots, f_{n-1}^{p^m-1}$ が一意的に求まるための必要十分条件は，自己同型作用素セル $\{\Phi_i(x)\}$ がたがいに独立なることである。

(証明略)

$p=2$, $m=1$, $k=1$ の場合を除いてこのような作用素セル（自己同型作用素）は必らず存在する。たとえば

$$\begin{cases} \Phi_0(x) = (1, 1, \cdots, 1) \\ \Phi_1(x) = (1, \varphi, \cdots, 1) \\ \quad\vdots \\ \Phi_{p^m-1}(x) = (1, 1, \cdots, \varphi) \end{cases}$$

はその自明な例である。この作用素と回路網との対応を調べてみる。（9）式は図4の回路網に対応する。変数 x_i について逐次次の手順を応用すれば任意の多出力回路網がカスケード合成できることになる。

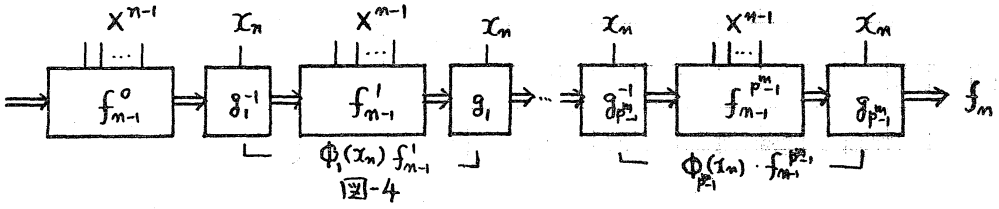


図-4

手順.（1）与えられた n 変数関数の k 組を E 七 F 表現する。

（2）適当な作用素に対応する標準方程式へ変換し、成分 $Q_0, Q_1, \cdots, Q_{p^m-1}$ を求める。

（3）連立方程式

$$Q_0 = g_{00} f^0_{n-1} \oplus g_{01} f^1_{n-1} \oplus \cdots \oplus g_{0p^m-1} f^{p^m-1}_{n-1}$$

$$Q_1 = g_{10} f^0_{n-1} \oplus g_{11} f^1_{n-1} \oplus \cdots \oplus g_{1p^m-1} f^{p^m-1}_{n-1}$$

$$\vdots$$

$$Q_{p^m-1} = g_{p^m-1,0} f_{m-1}^{0} \oplus g_{p^m-1,1} f_{m-1}^{1} \oplus \cdots \oplus g_{p^m-1,p^m-1} f_{m-1}^{p^m-1}$$

より $f_{m-1}^{0}, f_{m-1}^{1}, \cdots, f_{m-1}^{p^m-1}$ を求める。

(3) 各成分 f_{m-1}^{i} に同様の手順を応用する。

(4) 全成分が一変数関数になれば終了。

最終的に求まった多項式は一変数関数で $\alpha_i x^{\varepsilon_i}$ の形の項の一次結合となっている。従って前述のことよりこれらは x^{ε_i} を入力とするセルのカスケードになるが、係数と入力条件との関係が $GF(p)$ の場合と異なる。これについてのべよう。

$\alpha_i \in GF(p^m)$ は m 個の加法に関する生成元をもっている。この生成元を $\{g_1, g_2, \cdots, g_m\}$ とする。すると

$\forall \alpha \in GF(p^m)$

$$\alpha = \alpha_1 g_1 \oplus \alpha_2 g_2 \oplus \cdots \oplus \alpha_m g_m, \quad \alpha_j \in GF(p).$$

故にセルへの入力としては $g_i x^{\varepsilon_i}$ の形を認めなければならない。

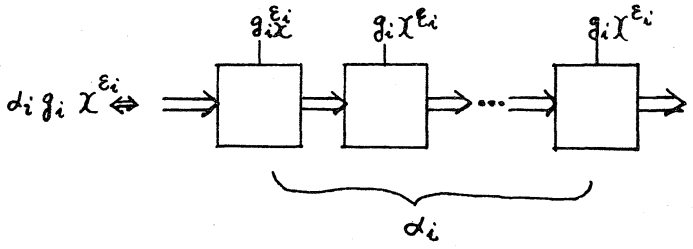


図 5

定理.7 任意の p^m 値 k 出力回路網は $p=2,\ m=1,\ k=1$ の場合を除いて高々 $k+2(p^m-1)$ 種のセルを用いて，所要セル数 $L_n < km(p^{mn+1}-p^{mn})+2p^{m(n-1)}-2$ で合成可能である。

（証明）前半は標準セル k 種，作用素セル $2(p^m-1)$ 種より明らか。個数は合成方法より $L_n = p^m L_{n-1} + 2(p^m-1)$

$= (p^m)^2 L_{n-2} + 2p^m(p^m-1) + 2(p^m-1) = \cdots$

$= (p^m)^{n-1} L_1 + 2(p^m-1)((p^m)^{n-2} + \cdots + 1)$

$= p^{m(n-1)} L_1 + 2p^{m(n-1)} - 2$

$L_1 < km(p^{m+1}-p^m)$ より

$L_n < (km(p^{m+1}-p^m)+2)p^{m(n-1)} - 2$

$= km(p^{mn+1}-p^{mn}) + 2p^{m(n-1)} - 2$

（証明終）

以上 $GF(p^m)^k$ の演算での合成可能性についてのべてきたが，$m=1$ の場合には入力条件が異なり定理7は次のようになる；

系.1 k 出力回路網 $f: X^n \to GF(p)^k$ は $p=2,\ k=1$ の場合を除けば，高々 $(2p+k-2)$-種の1入力セルを用いて常に合成可能であり所要セル数は

$$L_n \leq k(p^{n+1}-p^n) + 2\cdot p^{n-1} - 2$$

（証明略）

例題. 3　次の関数を合成せよ。

x_2 x_1	f
0 0	1
0 1	ρ_1
0 ρ_1	0
0 ρ_2	ρ_2
1 0	0
1 1	0
1 ρ_1	0
1 ρ_2	ρ_1
ρ_1 0	0
ρ_1 1	ρ_2
ρ_1 ρ_1	0
ρ_1 ρ_2	ρ_2
ρ_2 0	1
ρ_2 1	0
ρ_2 ρ_1	0
ρ_2 ρ_2	0

$\varphi \cdot \rho = \rho_1 \cdot \rho$ なる作用素を用いる。

$$\begin{cases} \Phi_0(x) = (1, 1, 1, 1) \\ \Phi_1(x) = (1, \varphi, 1, 1) \\ \Phi_2(x) = (1, 1, \varphi, 1) \\ \Phi_3(x) = (1, 1, 1, \varphi) \end{cases}$$

とすると標準方程式は

$$\begin{cases} Q_0 = f_{m-1}^0 \oplus f_{m-1}^1 \oplus f_{m-1}^2 \oplus f_{m-1}^3 \\ Q_1 = f_{m-1}^0 \oplus \rho_2 f_{m-1}^1 \oplus \rho_1 f_{m-1}^2 \oplus f_{m-1}^3 \\ Q_2 = f_{m-1}^0 \oplus \rho_2 f_{m-1}^1 \oplus f_{m-1}^2 \oplus \rho_1 f_{m-1}^3 \\ Q_3 = f_{m-1}^0 \oplus \rho_2 f_{m-1}^1 \oplus \rho_2 f_{m-1}^2 \oplus \rho_2 f_{m-1}^3 \end{cases}$$

これより

$$\begin{cases} f_{m-1}^0 = \rho_1 Q_0 \oplus \rho_2 Q_3 \\ f_{m-1}^1 = \rho_2 Q_0 \oplus \rho_1 Q_1 \oplus \rho_1 Q_2 \oplus \rho_2 Q_3 \\ f_{m-1}^2 = \rho_2 Q_1 \oplus Q_2 \oplus \rho_1 Q_3 \\ f_{m-1}^3 = Q_1 \oplus \rho_2 Q_2 \oplus \rho_1 Q_3 \end{cases}$$

まず f_2 を展開すると

$$f_2(x_1, x_2) = \rho_2 x_1^3 x_2^3 \oplus x_1^3 x_2^2 \oplus \rho_1 x_1 x_2^3 \oplus \rho_2 x_1^2 x_2^2 \oplus \rho_1 x_1^2 x_2$$
$$\oplus \rho_2 x_1 \oplus \rho_1 x_1 x_2 \oplus \rho_2 x_2^2 \oplus \rho_1 x_2 \oplus 1$$

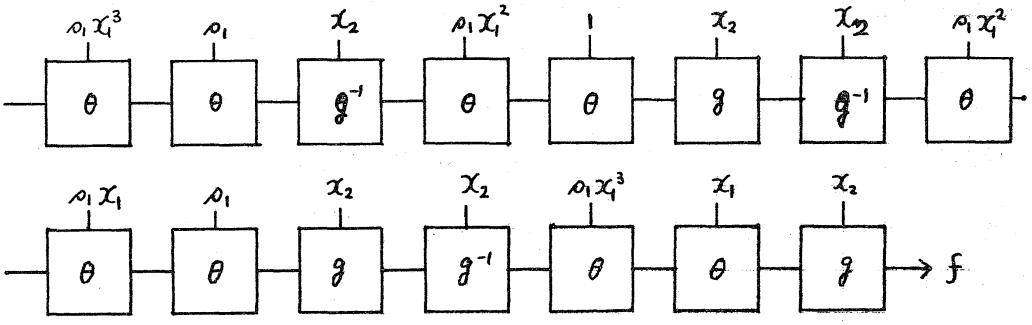
これより　$Q_0 = 1 \oplus \rho_2 x_1$,　$Q_1 = \rho_1 x_1^2 \oplus \rho_1 x_1 \oplus \rho_1$

$Q_2 = x_1^3 \oplus \rho_2 x_1^2 \oplus \rho_2$　$Q_3 = \rho_2 x_1^3 \oplus \rho_1 x_1$

故に　$f^0 = \rho_1 x_1^3 \oplus \rho_1$,　$f^1 = \rho_1 x_1^2 \oplus 1$

$f^2 = \rho_1 x_1^2 \oplus \rho_1 x_1 \oplus \rho_1$,　$f^3 = \rho_1 x_1^3 \oplus x_1$

従って次の回路網を得る：



同様に p 値論理関数の場合には回路網の rail state X^k K 位数 p^k の巡回群の演算 C_{p^k} を定義すれば類似の議論を進めることができる。主な結果を証明なしで示す。

定理.8　k 出力回路網 $f: X^n \to C_{p^k}$ は $p=2, k=1$ でないなら，p 種の 1 入力セルを用いれば常に合成可能で所要セル数は $L_m \leq (p^{k+1} - p + 2) \cdot p^{n-1} - 2$

系.2.　$p \neq 2$ とすると任意の回路網 $f: X^n \to C_p$ は 1 入力セルのカスケードで常に合成可能で所要セル数は

$$L_m \leq (p^2 - p + 2) \cdot p^{n-1} - 2$$

鈴木[7,8,9]らによって $p=2$, $k=1$ の場合は1入力セルは不能ではないことが示された。従って表2より3値セルが任意のブール関数を合成する意味で完備な最簡セルであると言える。次に問題になるのは今までのカスケード合成で用いたセルをある基本的なセルで置換できないかということである。一般 p^m 値関数の場合は未解決であるが $p=2,3$ の場合には次の結果が成りたつ：

定理.9. 2値又は3値多出力回路網は1種のセルのカスケードで合成することができる。[6]

結言. $GF(p^m)$ の演算で定義された多値論理関数のカスケード合成の問題を純代数的に取り扱かった。その結果ELF表現とその表現上に定義される作用素の概念を用いれば任意の多出力回路網が1入力セルのカスケードで実現可能である：とが示された。この手法は $GF(p)$ の演算で定義された多値関数の合成理論の一般化であるが、それに伴って入力条件のように若干の今までと異った性質が明らかになった。又この一般化によってこの手法が H として全ての有限体の演算を有する場合に成立することが分った。最後にこの研究の初期の段階で有益な討論いただいた現在静岡大学の鈴木清之氏に深謝する。

[参考文献]

[1] Elspas and Stone : Decomposition of group functions and the synthesis of multirail cascades. IEEE 8-th annual symp. on Swithing and Automata theory. 1967

[2] M. Yoeli : A group theoretical approach to two-rail cascades. IEEE. EC-14. 6 (Dec. 1965)

[3]. R.C. Minick : Cutpoint cellular logic. IEEE EC-13. 1964.

[4]. Maisil : The algebraic theory of switching circuits. Pergamon press. 1969.

[5]. 原尾. 鈴木. 野口. 大泉 ; 多出力多段論理回路網の合成. 信学論 52-C 昭44-09

[6] 原尾. 野口. 大泉 : 多段論理回路網による多値論理関数の合成. 信学論 54-C 昭46-2

[7]. 鈴木. 野口. 大泉. 多段論理回路網の構造に関する一考察. 信学論. 51-C 昭43-07.

[8] 鈴木. 野口. 大泉. (m+1, 1) 型多段論理回路網の性質と合成. 信学論. 52-C. 昭44-04.

[9] 鈴木. 野口. 大泉. (m+1, 1) 型多段論理網のブール関数実現能力. 信学論 52-C 昭44-08.

[10]. R.L. Herrmann : Selection and Implementation of Ternary Switching Algebra : Spring Joint Comp. Conf. 1968.